
Servidor de fitxers



Marc Serra <nandelbosc@s3os.net>

Copyright © 2005 Solucions i Serveis amb Sistemes Open Source (www.s3os.net)

En PEIXGLOBO serà el nostre servidor de fitxers.

Ens servirà fitxers tant a nivell local, a través de Samba, com a nivell extern, FTP (File transfer protocol)

Per a la tasca de servidor a nivell local hem escollit Samba enlloc del clàssic per a Linux NFS (Network File System), d'aquesta manera estem obrint els sistemes de Microsoft a un món molt més ampli, el de Linux

Per a el protocol de transferència de fitxers tenim una infinitat d'aplicacions: Proftpd, VSFTP, Pure-ftpd, oftpd, ... Ens hem quedat amb VSFTP per la seva facilitat de configuració i l'alt nivell de seguretat que ens ofereix.

Table of Contents

Samba	2
-------------	---

Instal·lació	2
Configuració	2
Usuaris	4
Engegada, parada, i prova	4
Exemple de configuració als clients	6
Samba com a PDC	6
VSFTP	8
Instal·lació	8
Configuració	8
Usuaris	9
Prova	10

Samba

Samba ens permet compartir carpetes a la xarxa, tant local com a internet. Aquesta última no és gaire recomanable, samba és un protocol on les contrasenyes no viatgen encriptades i l'informació que tenim pensat compartir, és suficientment important com per no córrer aquest risc.

Instal·lació

Comencem...

```
# emerge samba
```

Configuració

Un cop instal·lat donem un cop d'ull al següent fitxer de configuració (els comentaris són suficients):

```
peixglobo # cat /etc/samba/smb.conf
#####
# CONFIGURACIONS GLOBALS DEL SERVIDOR #
#####

[global]

    # nom del grup de treball
    workgroup = S3OS
    # nom netbios
    netbios name = <peixglobo>
    # nom del servidor, %v = versió
    server string = Samba Server %v
    # fitxer de logs, %m = machine (fitxer per cada màquina)
    log file = /var/log/samba3/log.%m
    # tamany màxim del fitxer
    max log size = 50
    # nivell de log, si tenim problemes el podem augmentar per depurar
    log level = 1
    # hosts permesos, la nostra LAN
    hosts allow = 192.168.0.0/24
    # nivell de seguretat
    security = user
    # encripta passwords al fitxers de contrasenyes
    encrypt passwords = yes
    # nom del fitxer de contrasenyes
    smb passwd file = /var/lib/samba/private/smbpasswd
    # opcions per a un bon rendiment
```

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
# a quina interfície escolatarà
interfaces = 192.168.0.2/24
# per defecte
os level = 33
# ja tenim DNS
dns proxy = no

#####
# RECURSOS COMPARTITS #
#####

# Disponible a tot el public, amb el nom 'media'
[media]
# comentari que veurem
comment = Media a la peixera (music, imatges, ...)
# quina és la carpeta
path = /mnt/disk2
# és pública, hi pot accedir tothom sense login
public = yes
# però no hi pot escriure ningú
writable = no
# excepte l'usuari 'nandelbosc'
write list = nandelbosc
# al explorar la xarxa ens mostrarà aquest recurs
browseable = yes
# no ens mostrarà els fitxers ocults (.nom.fitxer)
hide dot files = Yes
# no ens permet l'accés al fitxers que conténen: XXX o \\
#         acaben en .tmp
veto files = /*XXX*/*.tmp/

# Disponible per a programadors
[desenvolupament]
comment = Codis font, binaris, ...
path = /mnt/codi
# només hi ténen accés els usuaris del grup de programadors
valid users = @programers
# no és pública
public = no
# no s'hi pot escriure...
writable = no
# ...si no ets programador
write list = @programers
# al explorar la xarxa NO ens mostrarà aquest recurs
browseable = no
# força que els fitxers d'aquest directori siguin del grup \\
#         programers
force group = programers
# força els següents permisos (per fitxers)
force create mode = 0660
# força els següents permisos (per carpetes)
force directory mode = 0770

# Disponible per a programadors i dissenyadors
[webs]
comment = Webs d'S30S
path = /www
# només hi volem els dissenyadors i programadors
valid users = @dissenyadors, @programers
public = no
writable = no
write list = @dissenyadors, @programers
```

```
valid users = @dissenyadors, @programers
browseable = no
force create mode = 0660
force directory mode = 0770

# Disponible per a tot els usuaris d'S3OS
[varis]
comment = Fitxers varis per usuaris d'S3OS
valid users = @s3os
public = no
writable = no
write list = @S3os
browseable = yes
force group = s3os
force create mode = 0660
force directory mode = 0770
hide dot files = Yes
```

Usuaris

Hem parlat d'usuaris i grups, però com es fan? Amb la comanda 'smbpasswd'

Important

Els usuaris de samba han de tenir compte al sistema!

Crear usuaris

```
peixglobo # smbpasswd -a nandelbosc
New SMB password:
Retype new SMB password:
startsmbservice: file /var/lib/samba/private/smbpasswd \
did not exist. File successfully created.
Failed to initialise SAM_ACCOUNT for user nandelbosc. Does this \
user exist in the UNIX password database ?
Failed to modify password entry for user nandelbosc
```

Hem avisat, han de tenir compte al sistema... però no cal que tinguin 'home' ni 'shell'

```
peixglobo # adduser nandelbosc -d /dev/null -s /bin/false
peixglobo # smbpasswd -a nandelbosc
New SMB password:
Retype new SMB password:
Added user nandelbosc.
```

Esborrar usuaris

Si un membre deixa S3OS, ja no li cal compte, ni a samba, ni al sistema

```
peixglobo # smbpasswd -x nandelbosc
peixglobo # deluser nandelbosc
```

Enggada, parada, i prova

Engegar Samba

```
peixglobo # /etc/init.d/samba start
```

A l'inici

```
peixglobo # rc-update add samba default
```

Parar Samba

```
peixglobo # /etc/init.d/samba stop
```

Si només el volem reiniciar...

```
peixglobo # /etc/init.d/samba restart
```

Provant Samba

Podem fer-ho desde la mateixa màquina...

```
mandelbosc@peixglobo $ smbclient -L localhost
Password:
Anonymous login successful
Domain=[S3OS] OS=[Unix] Server=[Samba 3.0.10]

Sharename      Type      Comment
-----
media          Disk     Media a la peixera (music, imatges, ...)
varis         Disk     Fitxers varis per usuaris d'S3OS
Domain=[S3OS] OS=[Unix] Server=[Samba 3.0.10]

Server          Comment
-----
<PEIXGLOBO A S3OS>      Samba Server 3.0.10

Workgroup      Master
-----
S3OS
```

Hem llistat els recursos compartits que disposa l'usuari mandelbosc

Ara ens connectarem a la carpeta 'codi' amb l'usuari 'shadow'

```
peixglobo # smbclient //localhost/codi
Password:
Domain=[S3OS] OS=[Unix] Server=[Samba 3.0.10]
smb: \> ls
.          D          0   Sun May 22  \
18:59:01 2005
..         D          0   Thu Apr 21  \
```

```
                22:09:21 2005
shadow          D          0   Sun Jun  5  \\  
                18:28:39 2005
xevi            D          0   Wed May  4  \\  
                01:10:53 2005
```

```
47693 blocks of size 4194304. 34500 blocks available  
smb: \> exit
```

Finalment farem una connexió permanent. Muntarem la carpeta compartida /varis al directori local /home/nandelbosc/varis

```
nandelbosc@peixglobo # mkdir ~/varis  
nandelbosc@peixglobo # smbmount //localhost/varis /home/nandelbosc/varis \<\  
-o username=nandelbosc,password=XXXXXXXXXX
```

Exemple de configuració als clients

Si volem que els desktops ens mapegin els recursos a l'inici de la sessió d'usuari, hem d'afegir la següent línia al fitxer ~/.bash_profile:

```
nandelbosc@snoddesktop # echo>>smbmount //localhost/varis \<\  
/home/nandelbosc/varis -o username=nandelbosc,password=XXXXXXXXXX
```

Samba com a PDC

Primary Domain Controller (controlador primari de dominis), aquesta és una de les opcions de què disposa samba i que demostra la potència d'aquesta aplicació. És capaç d'acceptar connexions com a servidor de domini de treball, això significa que els usuaris Windows\$ ténen totes les configuracions, contrasenyes, fitxers personals,... als repositoris de samba

Note

No cal dir que a s3os.net no utilitzem aquesta opció.

Fitxer de configuració

```
# nano /etc/samba/smb.conf  
[global]  
workgroup = PDC  
netbios name = Snodserver  
passdb backend = tdbsam  
add user script = /usr/sbin/useradd -m %u  
delete user script = /usr/sbin/userdel -r %u  
add machine script = /usr/sbin/useradd -g pdc -s /dev/null -d \<\  
/dev/null -M %u  
logon script = scripts\%G.bat  
logon path = \\%L\Profiles\%U  
logon home = \\%L\%U  
domain logons = Yes  
os level = 35  
preferred master = Yes  
domain master = Yes
```

```
idmap uid = 15000-20000
idmap gid = 15000-20000

log file = /var/log/samba3/log.%m
log level = 1

[home]
comment = Directoris Personals
path = /home/%U
browseable = no
write list = %U

[public]
comment = Directori Public
path = /home/public
browseable = yes
write list = %U
guest ok = no
create mode = 0775
directory mask = 0775

[netlogon]
comment = Netlogons
path = /var/lib/samba/netlogon
browseable = no
guest ok = yes

[Profiles]
comment = Profiles
path = /var/lib/samba/profiles
read only = No
profile acls = Yes
```

Directoris

Millor que explicar el fitxer anterior, uns exemples:

Aquests són els fitxers que anirà a buscar el client per loggejar-se al PDC, segons el grup de l'usuari, utilitzarà l'un o l'altre (opció 'logon script = scripts\%G.bat')

```
snodserver root # ls /var/lib/samba/netlogon/scripts/
                grup1.bat          grup2.bat          grup3.bat
```

Aquest és el contingut d'un dels fitxers...

```
snodserver root # cat /var/lib/samba/netlogon/scripts/grup1.bat
net use h: \\192.168.0.x\home /persistent:no
net use p: \\192.168.0.x\public /persistent:no
```

En aquest cas, un usuari del grup 'grup1', se li mapejaràn les unitats 'h:' i 'p:'

Els profiles són els fitxers d'usuari de Window\$, aquests els trobem a:

```
snodserver root # ls /var/lib/samba/profiles/
                user1          user2          user3          user4          usert5
```

Contingut de l'usuari1:

```
snodserver root # ls /var/lib/samba/profiles/user1/
    Cookies                Entorno de red            Favoritos                 MenÃ° Inicio
    NTUSER.DAT              Reciente                  ntuser.dat.LOG           Datos de programa
    Escritorio              Impresoras                Mis documentos           Plantillas
    SendTo                  ntuser.ini
```

Clients

Com que es necessita el sistema operatiu propietari de Micro\$soft, no mostrarem pas per pas com configurar els clients, només sapigueu que heu d'investigar com fer que el host (PC) s'ajunti a un controlador de dominis i dir-li que aquest es diu 'PDC'. Suposo que després de tres o quatre hores, 7 o 8 reinicis del sistema i un ratolí destroçat ho aconseguireu.

VSFTP

Very Secure File Transfer Protocol (Protocol de transferència de fitxers molt segur), només amb el nom ja podem entendre que és un dels servidors FTP més segurs que podem trobar... esperem que així segueixi molt de temps! ;)

Instal·lació

Penseu que aquest servei depèn del dimoni 'xinetd'; si no el tenim instal·lat, la següent comanda ho farà per nosaltres...

```
# emerge vsftpd
```

Configuració

```
peixglobo # nano /etc/vsftpd/vsftpd.conf
# permetem FTP anònim? Si, sense password
anonymous_enable=YES
no_anon_password=YES

# on chrootem l'usuari anonymous
anon_root=/netshare/snod/

# els usuaris locals ténen accés al FTP
local_enable=YES

# podem bloquejar les comandes FTP d'escriptura, no en el nostre cas
write_enable=YES

# màscara per usuaris locals (per defecte 077)
#local_umask=022

# permetem als a anonymous pujar fitxers? si és que si,
# descomentem la següent línia, i creem una carpeta que
# l'usuari ftp pugui escriure-hi
#anon_upload_enable=YES

# si volem que l'anonymous pugui crear directoris
```

```
#anon_mkdir_write_enable=YES

# podem posar missatges per a cada directori
dirmessage_enable=YES

# les transferències s'originaran del port 20 (data-ftp)
connect_from_port_20=YES

# amb les següents opcions podem canviar el nom d'usuari concret \\  
    per al fitxers pujats
#chown_uploads=YES
#chown_username=whoever

# loggin? evidenment!
xferlog_enable=YES

# per tenir el log en 'standard ftpd xferlog format'
#xferlog_std_format=YES

# el destí del fitxer de log:
xferlog_file=/var/log/vsftpd/vsftpd.log

# timeout per sessió
#idle_session_timeout=600

# timeout per dades
#data_connection_timeout=120

# usuari sense permisos
nopriv_user=nobody

# missatge de benvinguda
ftpd_banner>Welcome to la peixera

# podem especificar un fitxer de mails bannejats, per evitar certs \\  
    atacs DoS
deny_email_enable=YES
# per defecte...
banned_email_file=/etc/vsftpd/vsftpd.banned_emails

# podem especificar una llista d'usuaris que seràn chrootats, però \\  
    si activem
# la següent directiva ('YES') la llista passa a ser d'usuaris que \\  
    no chrootem
chroot_list_enable=YES
# per defecte...
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list

hide_ids=YES
# llista d'usuaris permesos a connectar-se (/etc/vsftpd/vsftpd.user_list)
userlist_enable=YES
# llista d'usuaris denegats
userlist_deny=NO

# com a dimoni (passem d'xinetd)
background=YES
# sempre escoltant
listen=YES
```

Usuaris

Com hem dit, són usuaris de sistema, però també hem parlat de fitxers que els permetem o deneguem

l'accés i altres propietats... aquí els tenim:

```
peixglobo # cd /etc/vsftpd
peixglobo vsftpd # nano vsftpd.chroot_list
marc

peixglobo vsftpd # nano vsftpd.user_list
marc
shadow
anonymous
ftp

peixglobo vsftpd # nano vsftpd.banned_emails
personadolenta@hotmail.com
personaMOLTdolenta@hotmail.com
```

Prova

Podem provar-lo desde la mateixa màquina:

```
peixglobo / # ftp localhost
Connected to localhost.
220 Welcome to la peixera
Name (localhost:root): anonymous
530 Please login with USER and PASS.
SSL not available
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x   4 ftp      ftp      1192968 Apr 21 07:46  \
    distfiles
drwxr-xr-x   4 ftp      ftp           96 Feb 16 08:18  \
    grp
drwxrwxr-x   4 ftp      ftp           96 Dec 29 19:46  \
    iso
drwxr-xr-x   5 ftp      ftp      120 Jan 05 17:46  \
    snodconfigs
drwxrwxr-x   4 ftp      ftp           96 Dec 29 19:46  \
    snodconfigs_old
drwxr-xr-x   2 ftp      ftp      336 May 19 18:41  \
    snoddistfiles
-rwx-----   1 ftp      ftp           93 Jan 19 12:14  \
    syncdistfiles.sh
-rw-r--r--   1 ftp      ftp           44 Feb 14 08:45  \
    syncdistfiles2.sh
226 Directory send OK.
ftp> bye
221 Goodbye.
```

Funciona!

Finalment un exemple d'un usuari sense estar a la llista de chroot, per tant amb "molta llibertat"

```
peixglobo vsftpd # ftp localhost
Connected to localhost.
220 Welcome to la peixera
Name (localhost:root): nandelbosc
530 Please login with USER and PASS.
SSL not available
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp           48 May 25 11:46  \
      ftp
drwxrwxrwx    3 ftp      ftp           104 May 31 16:15  \
      nandelbosc
drwxrwxrwx    2 ftp      ftp           80 May 24 23:46  \
      usuari
226 Directory send OK.
ftp> bye
221 Goodbye.
```

Ja estem, només hem de pensar a obrir el port a en MUSCLU (el tallafocs)